гические процессы — это значит оградить их от любых несанкционированных воздействий информационного характера, которые создают возможность некорректного выполнения технологических процессов.

Список литературы

1. ГОСТ 34.003–1990 Автоматизированные системы. Термины и определения.

2. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31.

3. Positive Technologies: отчет об уязвимостях АСУ ТП за 2016 год. URL: http://www.safe-surf.ru.

УДК 004.056.53

И. В. Кротенко
Научный руководитель: канд. тех. наук, доц. А. С. Лучинин
Уральский федеральный университет, Екатеринбург

PLC-СИСТЕМЫ КАК СРЕДСТВО ОСУЩЕСТВЛЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Аннотация. Существуют различные области применения систем передачи информации по сети 220 В и множество технических решений на их основе. Примерами могут быть распределенные системы управления и учета в цехах, системах жизнеобеспечения зданий, системах складского хранения, средствах учета потребления электроэнергии, системах охранной и пожарной сигнализации. Существуют возможности реализации концепции «умного дома», в котором вся бытовая электроника объединена в единую информационную сеть с возможностью централизованного управления [1]. Однако структура информационных пакетов, передаваемых такими устройствами по сети, слабо изучена и различна в конкретных случаях у разных производителей таких устройств. Все это потенциально может быть использовано для несанкционированного доступа к информации [2].

Ключевые слова: информация; безопасность; передача информации; техническая защита информации; сеть 220 В; PLC; несанкционированный доступ к информации.

В устройствах PLC (Power Line Communication) используется технология OFDM (передача данных с использованием множества ортогональных поднесущих). Высокоскоростной поток данных разбирается на несколько относительно низкоскоростных потоков, каждый из которых передается на отдельной поднесущей частоте с последующим их объединением в один сигнал [3]. Реально используются 1536 поднесущих с выделением 84 наилучших в диапазоне 2–34 МГц.

Адаптеры работают на физическом уровне сетевой модели OSI. На физическом уровне используются несущие OFDM с интервалом 24,414 кГц, с несущими от 2 до 30 МГц. В зависимости от соотношения сигнал/шум система автоматически выбирает вид модуляции: BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM и 1024 QAM каждой поднесущей (рис. 1) [4].

В ходе экспериментальных исследований было установлено, что информационные посылки идут с частотой 25 Гц (период 40 мс). Длительность информационного пакета составляет около 400 мкс (рис. 2).

Производителем Tp-Link сетевых адаптеров PLC серии AV (в эксперименте использовались адаптеры AV200 Nano) реализована возможность подключения новых сетевых адаптеров к существующему комплекту для расширения сети. Каждый следующий адаптер подключается к одному из предыдущих. Это потенциально создает возможность НСД к такой PLC сети для обладателя такого же комплекта сетевых адаптеров или хотя одного такого устройства [5].

Проведено экспериментальное исследование возможности НСД к сети PLC. Установлено, что для осуществления скрытного подключения к сети злоумышленнику (речь идет о внутреннем нарушителе) необходимо иметь три таких адаптера. Например, в какой-то организации отсутствует подключение к сети Интернет, но реализована внутренняя локальная сеть для обмена данными между сотрудниками. Эта сеть реализована стандартными методами (напри-

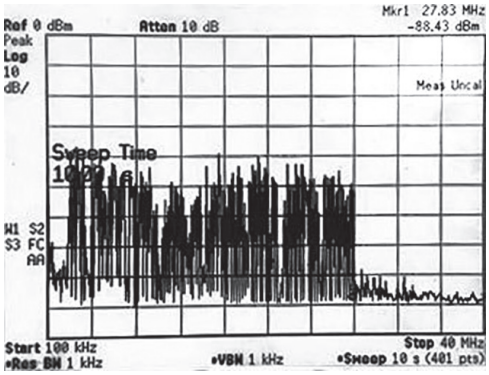

Рис. 1. Спектр сигнала, передаваемого через линию

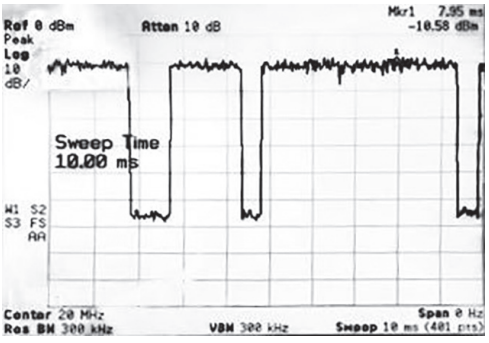

Рис. 2. Длительность информационных пакетов

мер, при помощи витой пары или оптоволоконной линии). Злоумышленник может скрытно подключить первый комплект адаптеров к участку этой сети (он просто меняет среду передачи данных) [6]. Косвенно это может быть заметно по изменению скорости передачи данных, если скорость передачи в сети организации выше, чем позволяют реализовать в сети 220 В сетевые адаптеры злоумышленника. В сети 220 В создается теневая сеть, распространяющаяся примерно на 300 м, как заявлено производителем. После этого злоумышленник может подключиться к этой сети третьим сетевым адаптером из удобного ему места в пределах допустимой дальности. Это подключение устанавливается автоматически в течение 60 с и не отображается в сети, но при этом злоумышленник, по сути, является равноправным участником сети и может наблюдать весь трафик с помощью сетевого перехватчика Wireshark. В перехватываемом трафике нарушитель может увидеть, в частности, IP-адрес отправителя и IP-адрес получателя, что позволит ему выдавать себя за определенного пользователя и стать легальным участником сети.

Производителем данного сетевого оборудования реализована возможность шифрования данных, передаваемых через сетевые адаптеры PLC. Это сделано с целью не допустить возможность несанкционированного подключения к чужой PLC сети из другой такой сети через единую электросеть 220 В, используя такое же оборудование. Но в случае описываемой атаки эта функция, наоборот, помогает нарушителю. Если он будет шифровать передаваемый в «его» сети трафик, то он усложнит задачу анализа своих действий после обнаружения НСД.

Главной мерой защиты от подобной атаки является проверка состояния коммуникаций, особенно на рабочих местах операторов ЭВМ и в смежных помещениях, в том числе в случае, если не установлены сетевые фильтры, или злоумышленник обходит их, оперируя в пределах контролируемой зоны. Важно обращать внимание, какие устройства включены в сеть на конкретных рабочих местах.

В работе экспериментально установлено, что описанный канал передачи можно закрыть с помощью подачи в сеть шумоподобного сигнала амплитудой более 8 В, но это работает только при попадании сигнала помехи на поднесущие OFDM в сигнале PLC. Важную роль играет равномерное распределение сигнала помехи по широкому участку частотного диапазона [7].

Список литературы

1. *Sharma K.*, *Saini L. M.* Power-line communications for smart grid: Progress, challenges, opportunities and status // Renewable and Sustainable Energy Reviews. September 2016. P. 705–751.

2. *Kaczmarczyk V.*, *Bradac Z.*, *Arm J.* An indoor positioning system based on NanoPAN modules // IFAC-PapersOnLine. 2015. P. 89–94.

3. *Sung Y.-S.*, *Lee J.-H.*, *Kim Y.-H.* Optimal subcarrier pairing scheme for maximal ratio combining in OFDM power line communications // International Journal of Electronics and Communications (AEÜ). April, 2014. P. 1–6.

4. *Охрименко В.* PLC-технологии // Электронные компоненты. 2009. № 10. С. 58–62.

5. *Хорев А. А.* Средства перехвата информации с проводных линий связи. М., 2008. 24 с.

6. *Хорев А. А.* Организация защиты информации от утечки по техническим каналам. Информационная система «Техника для спецслужб» // Бюро научно-технической информации, 2000. 13 с.

7. *Götz M.*, *Rapp M.*, *Dostert K.* Power Line Channel Characteristics and Their Effect on Communication System Design // IEEE Communications Magazine. April, 2004. P. 78–86.

УДК 53083

Д. М. Кучин, Д. А. Паршин
Научный руководитель: доц. К. И. Костромитин
Южно-Уральский государственный университет, Челябинск

ПРИМЕНЕНИЕ МЕТОДОВ ДЕСТРУКТИВНОГО ТЕСТИРОВАНИЯ, РЕНТГЕНОВСКОГО И ЛОГИЧЕСКОГО АНАЛИЗА ДЛЯ АНАЛИЗА РАБОТЫ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

Аннотация. Представлены характеристики и описание методов обнаружения аппаратных закладок на основе методов деструктивного тестирования, оптических методов контроля, рентгеновского и логического анализа цепей интегральных микросхем.

Актуальность исследования рентгеновских методов анализа заключается в том, что данные методы являются базовыми и наиболее распространенными при проверке печатных плат на наличие сторонних включений. Актуальность применения метода логического анализа заключается в том, что он теоретически позволяет получить все множество значений сигналов, получаемых при работе интегральной микросхемы, что может быть использовано для аппаратной защиты информации

Ключевые слова: деструктивное тестирование; оптические методы контроля; рентгеновский анализ; логический анализ.